UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/584,194	05/25/2007	Takehiro Ohkoshi	2565-0297PUS1	1262

2292 7590 01/26/2010
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2431	
NOTIFICATION DATE	DELIVERY MODE
01/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/584,194
Filing Date: May 25, 2007
Appellant(s): OHKOSHI ET AL.

D. Richard Anderson
Reg. No. 40,439
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed October 5, 2009 appealing from the Office action mailed April 3, 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2004/0034771	EDGETT	2-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-10 are rejected under 35 U.S.C. 102 (e) as being anticipated by Edgett et al. (U.S. Patent Pub. No. US 2004/0034771)

Regarding claim 1, Edgett discloses:

An authenticated device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device (paragraph 0057: *key index and algorithm are sent to the authentication server*);

a receiving unit to receive from the authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing unit to perform an authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Edgett discloses:

The authenticated device of claim 1,

wherein the memory unit stores at least one algorithm identifier and at least one encryption key identifier in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

wherein the transmitting unit transmits, to the authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile (paragraph 0057: *key index and algorithm are sent to the authentication server*);

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier paired as a prescribed profile, among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired as the prescribed profile received by the receiving unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Edgett discloses:

The authenticated device of claim 2,

wherein the memory unit further stores a version identifier to identify a version indicating a set in such a manner that one set is formed from at least one algorithm corresponding to the at least one algorithm identifier stored (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier*);

wherein the transmitting unit transmits the version identifier stored by the memory unit to the authenticating device (paragraph 0057: *key index and algorithm are sent to the authentication server*);

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier corresponding to a prescribed algorithm among the at least one algorithm forming the set indicated by the version identified by the version identifier transmitted from the transmitting unit (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier received by the receiving unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 4, Edgett discloses:

An authenticating device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier; a receiving unit to receive at least one algorithm identifier and at least one encryption key identifier from an authenticated device (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit (paragraph 0057: *key index and algorithm are stored in a private key database*), when the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit (paragraph 0057: *key index and algorithm are stored in a private key database*);

a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing unit to perform an authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Edgett discloses:

The authenticating device of claim 4,

wherein the memory unit stores at least one profile identifier to identify at least one profile, whereby one algorithm identifier among the at least one algorithm identifier and one encryption key identifier among the at least one encryption key identifier are paired (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

wherein the receiving unit further receives at least one profile identifier from the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

wherein the selecting unit selects a prescribed profile identifier to be stored by the memory unit from among the at least one profile identifier received by the receiving unit, when the at least one profile identifier stored by the memory unit exists among the at least one profile identifier received by the receiving unit (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

wherein the transmitting unit transmits the prescribed profile identifier selected by the selecting unit to the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired by a prescribed profile identified by the prescribed profile identifier transmitted by the transmitting unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Edgett discloses:

The authenticating device of claim 5,

wherein the memory unit further stores a version identifier to identify a version of a set in such a manner that one set is formed from at least one algorithm corresponding to the at least one algorithm identifier stored (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier*);

wherein the receiving unit further receives a prescribed version identifier from the authenticated device (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier and the update server supplies the version number*);

wherein the selecting unit selects the prescribed algorithm identifier corresponding to one algorithm in the set indicated by the version identified by the prescribed version identifier received by the receiving unit (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

wherein the transmitting unit transmits the prescribed algorithm identifier selected by the selecting unit to the authenticated device profile (paragraph 0057: *key index and algorithm are sent to the authentication server*); and wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier transmitted by the transmitting unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 7, Edgett discloses:

An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier and the update server supplies the version number*);

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device paragraph 0057: *key index and algorithm are sent to the authentication server*);

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 8, Edgett discloses:

An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a first receiving step to receive the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device by the first transmitting step, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier and the update server supplies the version number*);

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 9, Edgett discloses:

An authenticating method comprising:

transmitting, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier (paragraph

0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 10, Edgett discloses:

An authenticating method comprising:

transmitting, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

receiving the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier and the update server supplies the version number*);

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received (paragraph 0058: *password is decrypted and authenticated*).

(10) Response to Argument

The Appellant argues:

That Edgett does not teach or suggest a "receiving unit to receive a prescribed algorithm identifier and a prescribed encryption key identifier, which are selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit."

The Examiner first contends that Edgett teaches receiving a prescribed algorithm identifier selected from the at least one algorithm identifier and the at least one encryption key identifier. Edgett teaches a system of selecting between encryption key pairs and the underlying encryption/decryption algorithm (paragraph 0057). In order to select the algorithm to be used, Edgett discloses an algorithm identifier (paragraph 0058). This algorithm identifier is stored in a database, and is transmitted along with the key index (encryption key identifier) to the decryption server (paragraph 0058), which retrieves (selects) the correct algorithm associated with the algorithm identifier (paragraph 0058). The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) then sends which algorithm is to be employed in further communications and transmits the updated encryption key index and algorithm identifier back to the authenticated network user (authenticated device) (paragraph 0059) when the algorithm is updated (paragraph 0059).

The Examiner further contends that Edgett teaches receiving a prescribed encryption key identifier which is selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit. The public key and its corresponding key index are stored within the private key database of the dialer/network user (paragraph 0052). This key index is transmitted to the decryption server, and the decryption server uses the key index to retrieve (select) the appropriate key which is to be used in the authentication (paragraph 0052). The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) then sends the key with its associated key index to the network user when authenticated (authenticated network user) (paragraph 0055).

The Appellant further argues:

That Edgett does not teach transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to an authenticated device.

The Examiner contends that Edgett teaches transmitting the prescribed algorithm identifier to an authenticated device. The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) sends which algorithm is to be employed in further communications and transmits the updated encryption key index and algorithm identifier back to the authenticated network user (authenticated device) (paragraph 0059) when the algorithm is updated (paragraph 0059).

The Examiner further contends that Edgett teaches transmitting the prescribed key identifier to an authenticated device. The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) sends the key with its associated key index to the network user when authenticated (authenticated network user) (paragraph 0055).

The Appellant finally argues that:

Edgett does not teach transmitting and receiving a plurality of algorithm identifiers and a plurality of encryption key identifiers stored between an authenticating device and an authenticated device.

The Examiner contends that Edgett does teach transmitting and receiving a plurality of algorithm identifiers stored between an authenticating device and an authenticated device. Edgett teaches a system of selecting between encryption key pairs and the underlying encryption/decryption algorithm (paragraph 0057). In order to select the algorithm to be used, Edgett discloses an algorithm identifier (paragraph

0058). This algorithm identifier is stored in a database, and is transmitted along with the key index (encryption key identifier) to the decryption server (paragraph 0058), which retrieves (selects) the correct algorithm associated with the algorithm identifier (paragraph 0058). The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) then sends which algorithm is to be employed in further communications and transmits the updated encryption key index and algorithm identifier back to the authenticated network user (authenticated device) (paragraph 0059) when the algorithm is updated (paragraph 0059). The algorithm identifiers in this case are one of many that are transmitted back and forth between the network user (authenticated device) and the Server (decryption/update servers) (authenticating device) as there is both an old algorithm and a new algorithm (plurality of algorithms) and they can overlap until the user is migrated (paragraphs 0058-0059). Therefore, the algorithm identifier serves the purpose of identifying which algorithm, old or new, is supposed to be used in the encryption/decryption process to be carried out between the user and the Servers.

The Examiner further contends that Edgett does teach transmitting and receiving a plurality of encryption key identifiers stored between an authenticating device and an authenticated device. The public key and its corresponding key index are stored within the private key database of the dialer/network user (paragraph 0052). This key index is transmitted to the decryption server, and the decryption server uses the key index to retrieve (select) the appropriate key which is to be used in the authentication (paragraph 0052). The Update Server, which together with the decryption server comprises the authenticating device (both functionalities can be housed on the same device/server) then sends the key with its associated key index to the network user when authenticated (authenticated network user) (paragraph 0055). Edgett discloses that there is a plurality of overlapping key pairs which may each be defined by a key index (key identifier) (paragraph 0053). Therefore, the key index allows the decryption server to select which one of the overlapping key pairs is to be used in the encryption/decryption process (paragraph 0052). Therefore, the Examiner contends that there are a plurality of encryption key identifiers being transmitted between the authenticating device and the authenticated device.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KA

12/30/2009

Conferees:

William Korzuch

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431

Christopher Revak

/Christopher A. Revak/

Primary Examiner, Art Unit 2431